Notice of Allowability	Application No.	Applicant(s)	
	09/928,266	SOLINAS, JEROME ANTHONY	
	Examiner	Art Unit	
	Tamara Teslovich	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *application filed on 08/09/01*.

2. ☒ The allowed claim(s) is/are *1-5*.

3. ☒ The drawings ~~filed on~~ *included by Examiner's Amendment* are accepted by the Examiner.

4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

6. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

7. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☒ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date 08/09/01
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date ~~01.14.05~~ Attached
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

Andrew Caldwell

ANDREW CALDWELL
SUPERVISORY PATENT EXAMINER

DETAILED ACTION

Allowable Subject Matter

Claims 1-5 are allowed.

The following is an examiner's statement of reasons for allowance:

As per claim 1, the prior art of record does not teach or suggest a combination as claimed, in which the modulus p is selected from the group of equations as specified in step (a), to be utilized in the method for identifying users, described in steps (b) through (o). The prior art described in page 6 of applicant's *Background of the Invention* discloses the use of a class of numbers in the form of 2^q-C chosen to create a more efficient modular reduction, to be utilized in a method for identifying users. At the time of the invention, there would be no motivation for a person of ordinary skill in the art to use the applicant's combination. Therefore, claim 1 is allowable.

Claims 2-5 are is allowable because they are dependent on allowable claim 1.

Interview Summary

Please refer to the Examiner's "Annotated Marked-Up Drawings" included as pages 3-6 of this office action for changes made to Figures 1-3, 5, and 6 as per Attorney's request.

"ANNOTATED MARKED-UP DRAWING"

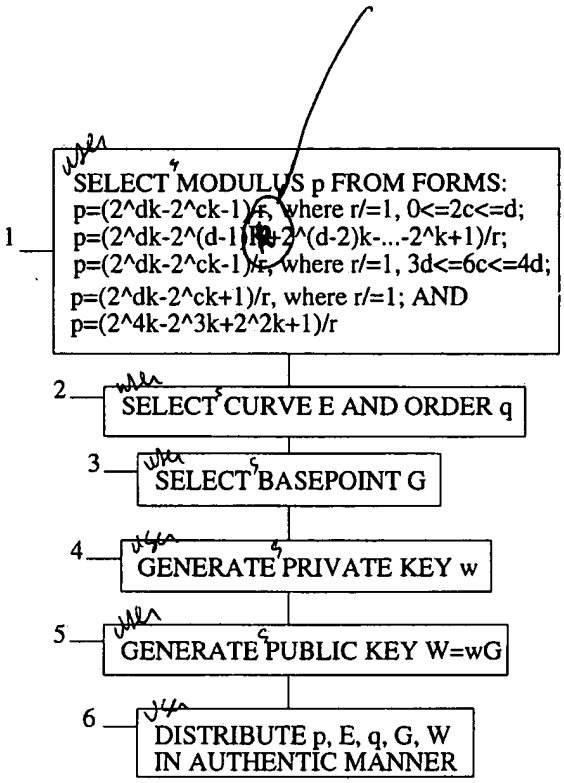

FIG. 1

"ANNOTATED MARKED-UP DRAWING"

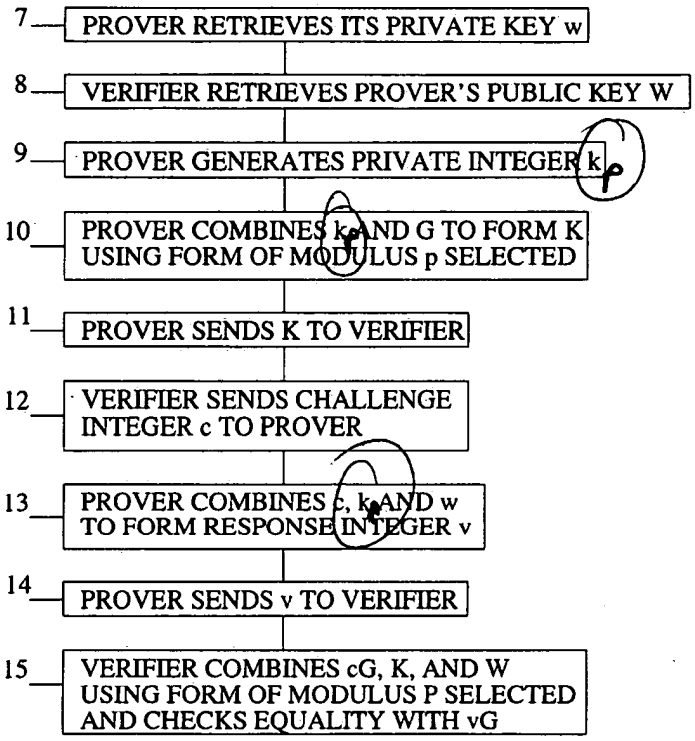

FIG. 2

"ANNOTATED ~~SHEET~~ MARKED-UP DRAWING"

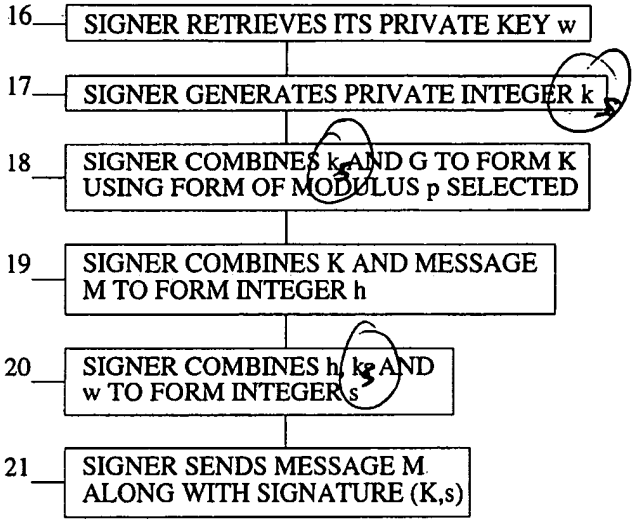

FIG. 3

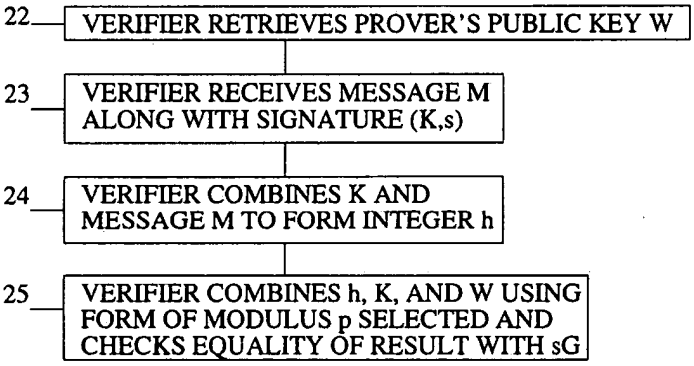

FIG. 4

"ANNOTATED MARKED-UP DRAWING"

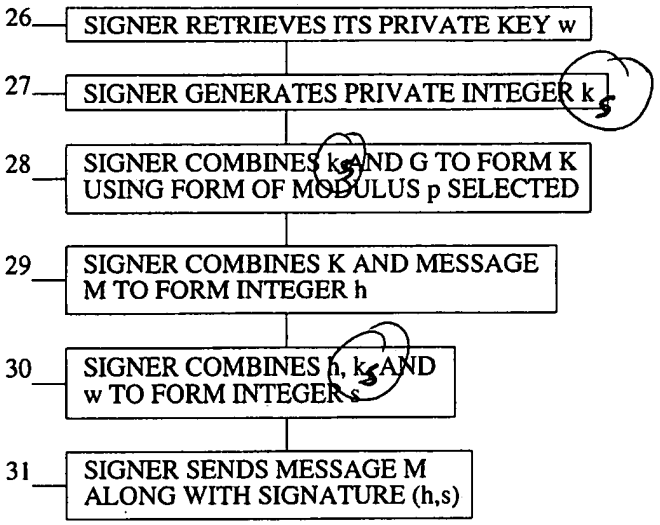

FIG. 5

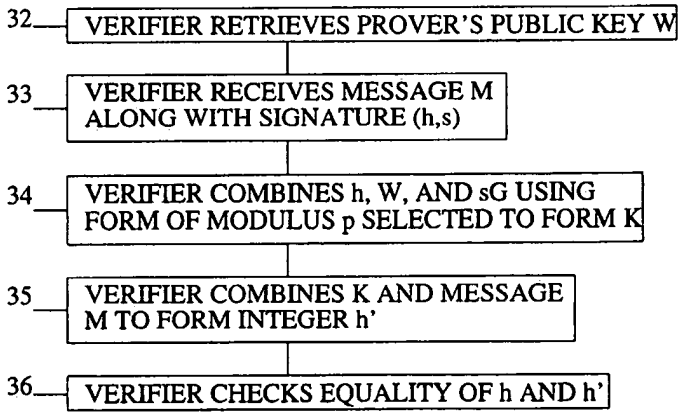

FIG. 6

EXAMINER'S AMENDMENT

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Attorney Robert D. Morelli on January 12, 2005.

Please amend Claims in accordance with Examiner's "Claim Amendments" included as pages 8-14 of this office action.

Please amend Specifications in accordance with Examiner's "Specification Amendments" included as pages 15-27 of this office action.

The following changes to the drawings have been approved by the examiner and agreed upon by applicant: Please replace Figures 1-6 with Examiner's "Replacement Sheet" Figures 1-6 as included in pages 28-31 of this office action.

CLAIM AMENDMENTS

Claim 1 (currently amended): A method of identifying a user, comprising the steps of:

a) selecting, by the user, a modulus *p* from the group of equations consisting of:

$$p=(2^{dk}-2^{ck}-1)/r,$$

where $0<2c<=d$, where *r* != does not equal 1, and where *GCD(c,d)*=1;

$$p=(2^{dk}-2^{(d-1)k}+2^{(d-2)k}-\ldots-2^{k}+1)/r,$$

where *d* is even, and where *k* is not equal to 2 (mod 4);

$$p=(2^{dk}-2^{ck}-1)/r,$$

where $3d<6c<4d$, and where *GCD(c,d)*=1;

$$p=(2^{dk}-2^{ck}+1)/r,$$

where $0<2c<=d$, where *r* != does not equal 1, and where *GCD(c,d)*=1; and

$$p=(2^{4k}-2^{3k}+2^{2k}+1)/r;$$

b) selecting, by the user, an elliptic curve E and an order q;

c) selecting, by the user, a basepoint G;

d) generating, by the user, a private key w;

e) generating, by the user, a public key $W=wG$;

f) distributing, by the user, p, E, q, G, and W in an authentic manner;

g) ~~retrieving~~ generating, by a prover, the prover's private key ~~w~~ w_p and public key W_p and distributing W_p;

h) retrieving, by a verifier, the prover's public key ~~W~~ W_p;

i) generating, by the prover, a private integer ~~k~~ k_p;

j) combining, by the prover, ~~k~~ k_p and ~~the prover's~~ G to form K using the form of the ~~prover's~~ modulus p;

k) sending, by the prover, K to the verifier;

l) sending, by the verifier, a challenge integer c to prover;

m) combining, by the prover, c, ~~k~~ k_p, and ~~w~~ w_p to form a response integer v;

n) sending, by the prover, v to the verifier; and

o) combining, by the verifier, cG, K, and ~~W~~ W_p using the form of the ~~prover's~~ modulus p and checking to see if the combination is equal to vG, if so the user is identified as the user, otherwise the user is not identified as the user.

Claim 2 (currently amended): The method of ~~generating a digital signature~~ claim 1, further comprising the steps of:

~~a) selecting a modulus *p* from the group of equations consisting of:~~

~~$p=(2^{dk}-2^{ck}-1)/r$,~~

~~where $0<2c<=d$, where $r /= 1$, and where $GCD(c,d)=1$;~~

~~$p=(2^{dk}-2^{(d-1)k}+2^{(d-2)k}-\ldots-2^{k}+1)/r$,~~

~~where d is even, and where k is not equal to 2 (mod 4);~~

~~$p=(2^{dk}-2^{ck}-1)/r$,~~

~~where $3d<6c<4d$, and where $GCD(c,d)=1$;~~

~~$p=(2^{dk}-2^{ck}+1)/r$,~~

~~where $0<2c<=d$, where $r /= 1$, and where $GCD(c,d)=1$; and~~

~~$p=(2^{4k}-2^{3k}+2^{2k}+1)/r$,~~

~~b) selecting an elliptic curve *E* and an order *q*;~~

~~c) selecting a basepoint *G*;~~

~~d) generating a private key *w*;~~

~~e) generating a public key *W=wG*;~~

~~f) distributing *p, E, q, G*, and *W* in an authentic manner;~~

~~g~~a) ~~retrieving~~ generating, by a signer, the signer's private key ~~*w*~~ w_S;

~~h~~b) generating, by the signer, a private integer ~~k~~ k_S;

~~i~~c) combining, by the signer, ~~k~~ k_S and *G* to form *K* using the form of the ~~prover's~~ modulus *p*;

~~j~~d) combining, by the signer, *K* and a message *M* to form an integer *h*;

~~k~~e) combining by the signer, *h,* ~~*k*~~ k_S, and ~~*w*~~ w_S to form an integer *s*; and

~~l~~f) sending, by the signer, *M* and (*K,s*) as a digital signature of *M*.

Claim 3 (currently amended): The method of claim ~~1~~ 2, further including the steps of:

a) retrieving, by the verifier, the prover's public key ~~*W*~~ W_p;

b) receiving, by the verifier, *M* and (*K,s*);

c) combining, by the verifier, *K* and *M* to form an integer *h*; and

d) combining, by the verifier, *h*, *k* K, and ~~W~~ W_p using the form of the ~~prover's~~ modulus *p* and checking to see if the combination is equal to *sG*, if so then the digital signature is verified, otherwise the digital signature is not verified.

Claim 4 (currently amended): The method of ~~generating a digital signature~~ claim 1, further comprising the steps of:

~~a) selecting a modulus *p* from the group of equations consisting of:~~

~~$p=(2^{dk}-2^{ck}-1)/r,$~~

~~where $0<2c<=d$, where $r /= 1$, and where $GCD(c,d)=1$;~~

~~$p=(2^{dk}-2^{(d-1)k}+2^{(d-2)k}-\ldots-2^{k}+1)/r,$~~

~~where *d* is even, and where *k* is not equal to 2 (mod 4);~~

~~$p=(2^{dk}-2^{ck}-1)/r,$~~

~~where $3d<6c<4d$, and where $GCD(c,d)=1$;~~

~~$p=(2^{dk}-2^{ck}+1)/r,$~~

~~where $0<2c<=d$, where $r /= 1$, and where $GCD(c,d)=1$; and~~

~~$$p=(2^{4k}-2^{3k}+2^{2k}+1)/r;$$~~

~~b) selecting an elliptic curve E and an order q;~~

~~c) selecting a basepoint G;~~

~~d) generating a private key w;~~

~~e) generating a public key $W=wG$;~~

~~f) distributing p, E, q, G, and W in an authentic manner;~~

~~g~~a) ~~retrieving~~ generating, by a signer, the signer's private key ~~w~~ w_S;

~~h~~b) generating, by the signer, a private integer ~~k~~ k_S;

~~i~~c) combining, by the signer, ~~k~~ k_S and G to form K using the form of the ~~prover's~~ modulus p;

~~j~~d) combining, by the signer, K and a message M to form an integer h;

~~k~~e) combining by the signer, h, ~~k~~ k_S, and ~~w~~ w_S to form an integer s; and

~~l~~f) sending, by the signer, M and (h,s) as a digital signature of M.

Claim 5 (currently amended): The method of claim 4, further including the steps of:

a) retrieving, by the verifier, the prover's public key ~~W~~ W_P;

b) receiving, by the verifier, *M* and (*h,s*);

c) combining, by the verifier, *h*, ~~*W*~~ $\underline{W_p}$, and *sG* using the form of the ~~prover's~~ modulus *p* to form *K*;

d) combining, by the verifier, *K* and *M* to form an integer *h'*; and

e) checking, by the verifier, that *h* is equal to *h'*, if so then the digital signature is verified, otherwise the digital signature is not verified.

SPECIFICATION AMENDMENTS

(Replace third full paragraph on page 2 with the following paragraph.) The use of cryptographic key pairs was disclosed in U.S. Pat. No. 4,200,770, entitled "CRYPTOGRAPHIC APPARATUS AND METHOD." U.S. Pat. No. 4,200,770 also disclosed the application of key pairs to the problem of key agreement over an insecure communication channel. The algorithms specified in this U.S. Pat. No. ~~4,200,700~~ 4,200,770 rely for their security on the difficulty of the mathematical problem of finding a discrete logarithm. U.S. Pat. No. 4,200,770 is hereby incorporated by reference into the specification of the present invention.

(Replace the first full paragraph on page 7 with the following paragraph.) It is an object of the present invention to efficiently create a digital signature using a modulus *p* selected from the following families of equations:

$$p=(2^{dk}-2^{ck}-1)/r,$$

where $0<2c<=d$, where r /= does not equal to 1, and where $GCD(c,d)=1$, where *GCD* is a function that returns the greatest common denominator between the variables in parenthesis;

$$p=(2^{dk}-2^{(d-1)k}+2^{(d-2)k}-\ldots-2^{k}+1)/r,$$

where *d* is even, and where *k* is not equal to 2 (mod 4);

$$p=(2^{dk}-2^{ck}-1)/r,$$

where $3d<6c<4d$, and where $GCD(c,d)=1$;

$$p=(2^{dk}-2^{ck}+1)/r,$$

where $0<2c<=d$, where r != does not equal to 1, and where $GCD(c,d)=1$; and

$$p=(2^{4k}-2^{3k}+2^{2k}+1)/r.$$

(Replace the first full paragraph on page 8 with the following paragraph.) The first step through sixth step are done by each user who wishes to have its message digitally signed. The first step is selecting a modulus p from the following family of equations:

$$p=(2^{dk}-2^{ck}-1)/r,$$

where $0<2c<=d$, where r != does not equal to 1, and where $GCD(c,d)=1$;

$$p=(2^{dk}-2^{(d-1)k}+2^{(d-2)k}-\ldots-2^{k}+1)/r,$$

where d is even, and where k is not equal to 2 (mod 4);

$$p=(2^{dk}-2^{ck}-1)/r,$$

where $3d<6c<4d$, and where $GCD(c,d)=1$;

$$p=(2^{dk}-2^{ck}+1)/r,$$

where $0<2c<=d$, where r ~~!=~~ does not equal to 1, and where $GCD(c,d)=1$; and

$$p=(2^{4k}-2^{3k}+2^{2k}+1)/r.$$

(Replace the sixth full paragraph on page 9 with the following paragraph.) The seventh step through fifteenth step are done to identity the user who wishes to have a message digitally signed. The seventh step is a prover ~~retrieving~~ generating its private key ~~w~~ w_p and public key $W_p=w_pG$, and distributing its W_p.

(Replace the seventh full paragraph on page 9 with the following paragraph.) The eighth step is a verifier retrieving the prover's public key ~~W~~ W_p.

(Replace the eighth full paragraph on page 9 with the following paragraph.) The ninth step is the prover generating a private integer ~~k~~ k_p.

(Replace the ninth full paragraph on page 9 with the following paragraph.) The tenth step is the prover combining ~~*k*~~ $\underline{k_p}$ and ~~prover's~~ *G* to form *K* using the form of the ~~prover's~~ modulus *p*.

(Replace the twelfth full paragraph on page 9 with the following paragraph.) The thirteenth step is the prover combining *c*, ~~*k*~~ $\underline{k_p}$, and ~~*w*~~ $\underline{w_p}$ to form a response integer *v*.

(Replace the fourteenth full paragraph on page 9 with the following paragraph.) The fifteenth step is the verifier combining *cG*, *K*, and ~~*W*~~ $\underline{W_p}$ using the form of the ~~prover's~~ modulus *p* and checking to see if the combination is equal to *vG*. If the combination is equal to *vG* then the prover is properly identified. Otherwise, the prover is not properly identified.

(Replace the fifteenth full paragraph on page 9 with the following paragraph.) The sixteenth step through the twenty-first step are done by the person digitally signing a message. The sixteenth step is a signer ~~retrieving~~ generating its private key ~~*w*~~ $\underline{w_S}$.

(Replace the sixteenth full paragraph on page 9 with the following paragraph.) The seventeenth step is the signer generating a private integer ~~*k*~~ $\underline{k_S}$.

(Replace the seventeenth full paragraph on page 9 with the following paragraph.) The eighteenth step is the signer combining ~~*k*~~ $\underline{k}_S$ and *G* to form *K* using the form of the ~~prover's~~ modulus *p*.

(Replace the second full paragraph on page 10 with the following paragraph.) The twentieth step is the signer combining *h*, ~~*k*~~ $\underline{k}_S$, and ~~*w*~~ $\underline{w}_S$ to form an integer *s*.

(Replace the fourth full paragraph on page 10 with the following paragraph.) The twenty-second step through the twenty-fifth step are done by the person verifying the digital signature. The twenty-second step is the verifier retrieving the prover's public key ~~*W*~~ $\underline{W}_p$.

(Replace the seventh full paragraph on page 10 with the following paragraph.) The twenty-fifth step is the verifier combining *h*, ~~*k*~~ $\underline{K}$, and ~~*W*~~ $\underline{W}_p$ using the form of the ~~prover's~~ modulus *p* and checking to see if the combination is equal to *sG*. If so, then the digital signature is verified. Otherwise, the digital signature is not verified.

(Replace the eighth full paragraph on page 10 with the following paragraph.) The twenty-sixth step through the thirty-first step are alternative steps for digitally signing a message. The twenty-sixth step is a signer retrieving its private key ~~*w*~~ $\underline{w}_S$.

(Replace the ninth full paragraph on page 10 with the following paragraph.) The twenty-seventh step is the signer generating a private integer ~~*k*~~ $\underline{k_S}$.

(Replace the tenth full paragraph on page 10 with the following paragraph.) The twenty-eighth step is the signer combining ~~*k*~~ $\underline{k_S}$ and *G* to form *K* using the form of the ~~prover's~~ modulus *p*.

(Replace the twelfth full paragraph on page 10 with the following paragraph.) The thirtieth step is the signer combining *h*, ~~*k*~~ $\underline{k_S}$, and ~~*w*~~ $\underline{w_S}$ to form an integer *s*.

(Replace the thirteenth full paragraph on page 10 with the following paragraph.) The ~~thirty-second~~ thirty-first step through thirty-sixth steps are alternative steps for verifying the digital signature of the alternative signing steps. The thirty-first step is the signer sending the message *M* and the digital signature (*h*,*s*) of *M*.

(Replace the fourteenth full paragraph on page 10 with the following paragraph.) The thirty-second step is the verifier retrieving the prover's public key ~~*W*~~ $\underline{W_p}$.

(Replace the first full paragraph on page 11 with the following paragraph.)

The thirty-fourth step is the verifier combining *h*, ~~*W*~~ *W*$_p$, and *sG* using the form of the ~~prover's~~ modulus *p* to form *K*.

(Replace the last paragraph on page 11 with the following paragraph.)

The present invention is a method of identifying a user, generating a digital signature for a message of the user, and verifying the digital signature in an efficient manner (i.e., in fewer steps than the prior art) using a modulus *p* selected from the following family of equations:

$$p=(2^{dk}-2^{ck}-1)/r,$$

where $0<2c<=d$, where r ~~!=~~ does not equal 1, and where $GCD(c,d)=1$;

$$p=(2^{dk}-2^{(d-1)k}+2^{(d-2)k}-\ldots-2^{k}+1)/r,$$

where *d* is even, and where *k* is not equal to 2 (mod 4);

$$p=(2^{dk}-2^{ck}-1)/r,$$

where $3d<6c<4d$, and where $GCD(c,d)=1$;

$$p=(2^{dk}-2^{ck}+1)/r,$$

where $0<2c<=d$, where r /= does not equal 1, and where $GCD(c,d)=1$; and

$$p=(2^{4k}-2^{3k}+2^{2k}+1)/r.$$

(Replace the last paragraph on page 13 with the following paragraph.) The first step 1 of the present method is selecting a modulus p from the following family of equations:

$$p=(2^{dk}-2^{ck}-1)/r,$$

where $0<2c<=d$, where r /= does not equal 1, and where $GCD(c,d)=1$;

$$p=(2^{dk}-2^{(d-1)k}+2^{(d-2)k}-\ldots-2^{k}+1)/r,$$

where d is even, and where k is not equal to 2 (mod 4);

$$p=(2^{dk}-2^{ck}-1)/r,$$

where $3d<6c<4d$, and where $GCD(c,d)=1$;

$$p=(2^{dk}-2^{ck}+1)/r,$$

where $0<2c<=d$, where r /= does not equal 1, and where $GCD(c,d)=1$; and

$$p=(2^{4k}-2^{3k}+2^{2k}+1)/r.$$

(Replace the seventh full paragraph on page 14 with the following paragraph.) The seventh step 7 of the method is a prover ~~retrieving~~ generating its private key ~~w~~ w_p and public key $W_p=w_pG$ and dirstibuting W_p.

(Replace the eighth full paragraph on page 14 with the following paragraph.) The eighth step 8 of the present method is a verifier retrieving the prover's public key ~~W~~ W_p.

(Replace the ninth full paragraph on page 14 with the following paragraph.) The ninth step 9 of the present method is the prover generating a private integer ~~k~~ k_p.

(Replace the first full paragraph on page 15 with the following paragraph.) The tenth step 10 of the present method is the prover combining ~~k~~ k_p and prover's G to form K using the form of the ~~prover's~~ modulus p.

(Replace the third full paragraph on page 15 with the following paragraph.) The twelfth step 12 of the present method is the verifier sending a challenge integer c to the prover.

(Replace the fourth full paragraph on page 15 with the following paragraph.) The thirteenth step 13 of the present method is the prover combining *c*, *k* $\underline{k_p}$, and ~~*w*~~ $\underline{w_p}$ to form a response integer *v*.

(Replace the sixth full paragraph on page 15 with the following paragraph.) The fifteenth step 15 of the present method is the verifier combining *cG*, *K*, and ~~*W*~~ $\underline{W_p}$ using the form of the ~~prover's~~ modulus *p* and checking to see if the combination is equal to *vG*. If the combination is equal to *vG* then the prover is properly identified. Otherwise, the prover is not properly identified.

(Replace the eighth full paragraph on page 15 with the following paragraph.) The sixteenth step 16 of the present method is a signer retrieving its private key ~~*w*~~ $\underline{w_S}$.

(Replace the ninth full paragraph on page 15 with the following paragraph.) The seventeenth step 17 of the present method is the signer generating a private integer *k* $\underline{k_S}$.

(Replace the tenth full paragraph on page 15 with the following paragraph.) The eighteenth step 18 of the present method is the signer combining *k* $\underline{k_S}$ and *G* to form *K* using the form of the ~~signer's~~ modulus *p*.

(Replace the twelfth full paragraph on page 15 with the following paragraph.) The twentieth step 20 of the present method is the signer combining *h*, ~~*k*~~ k_S, and ~~*w*~~ w_S to form an integer *s*.

(Replace the second full paragraph on page 16 with the following paragraph.) The twenty-second step 22 of the present method is the verifier retrieving the prover's public key ~~*W*~~ W_p.

(Replace the fifth full paragraph on page 16 with the following paragraph.) The twenty-fifth step 25 of the present method is the verifier combining *h*, ~~*k*~~ *K*, and ~~*W*~~ W_p using the form of the ~~prover's~~ modulus *p* and checking to see if the combination is equal to *sG*. If so, then the digital signature is verified. Otherwise, the digital signature is not verified.

(Replace the seventh full paragraph on page 16 with the following paragraph.) The twenty-sixth step 26 of the present method is a signer retrieving its private key ~~*w*~~ w_S.

(Replace the eighth full paragraph on page 16 with the following paragraph.) The twenty-seventh step 27 of the present method is the signer generating a private integer ~~*k*~~ k_S.

(Replace the ninth full paragraph on page 16 with the following paragraph.) The twenty-eighth step 28 of the present method is the signer combining ~~*k*~~ $\underline{k_S}$ and *G* to form *K* using the form of the ~~signer's~~ modulus *p*.

(Replace the eleventh full paragraph on page 16 with the following paragraph.) The thirtieth step 30 of the present method is the signer combining *h*, ~~*k*~~ $\underline{k_S}$, and ~~*w*~~ $\underline{w_S}$ to form an integer *s*.

(Replace the second full paragraph on page 17 with the following paragraph.) The thirty-second step 32 of the present method is the verifier retrieving the prover's public key ~~*W*~~ $\underline{W_p}$.

(Replace the fourth full paragraph on page 17 with the following paragraph.) The thirty-fourth step 34 of the present method is the verifier combining *h*, ~~*W*~~ $\underline{W_p}$, and *sG* using the form of the ~~prover's~~ modulus *p* to form *K*.

(Replace the first full paragraph on page 24 with the following paragraph.) A method of identifying user, generating digital signature, and verifying digital signature by selecting a modulus *p* in the form of $p=(2^{dk}-2^{ck}-1)/r$; $p=(2^{dk}-2^{(d-1)k}+2^{(d-2)k}-\ldots-2^{k}+1)/r$; $p=(2^{dk}-2^{ck}-1)/r$; $p=(2^{dk}-2^{ck}+1)/r$; and $p=(2^{4k}-2^{3k}+2^{2k}+1)/r$; selecting an elliptic curve *E* and an order *q*; selecting a basepoint *G*; generating a private key *w*; generating a public key *W*=*wG*; distributing *p*, *E*, *q*, *G*, and *W* to at least a

prover, a verifier, and a signer; ~~retrieving~~ generating ~~a~~ the prover's private key ~~*w*~~ w_p and public key $W_p=w_pG$; retrieving the prover's public key ~~*W*~~ W_p; generating a private integer ~~*k*~~ k_p; combining ~~*k*~~ k_p and ~~the prover's~~ *G* to form *K* using ~~the prover's modulus~~ *p*; sending *K* to the verifier; sending a challenge integer *c* to the prover; combining *c*, ~~*k*~~ k_p, and ~~*w*~~ w_p to form a response integer *v*; sending *v* to the verifier; combining *cG*, *K*, and ~~*W*~~ W_p using ~~the prover's modulus~~ *p* and checking to see if the combination is equal to *vG*. If not so, stop. Otherwise, ~~retrieving~~ generating, by the signer, the signer's private key ~~*w*~~ w_S; generating a private integer ~~*k*~~ k_S; combining ~~*k*~~ k_S and *G* to form *K* using ~~the prover's modulus~~ *p*; combining *K* and a message *M* to form an integer *h*; combining *h*, ~~*k*~~ k_S, and ~~*w*~~ w_S to form an integer *s*; sending *M* and (*K*,*s*) as a digital signature of *M*; retrieving ~~the prover's public key~~ ~~*W*~~ W_p; receiving *M* and (*K*,*s*); combining *K* and *M* to form an integer *h*; and combining *h*, ~~*k*~~ *K*, and ~~*W*~~ W_p using ~~the prover's modulus~~ *p* and checking to see if the combination is equal to *sG*. If so, the digital signature is verified.

"REPLACEMENT SHEET"

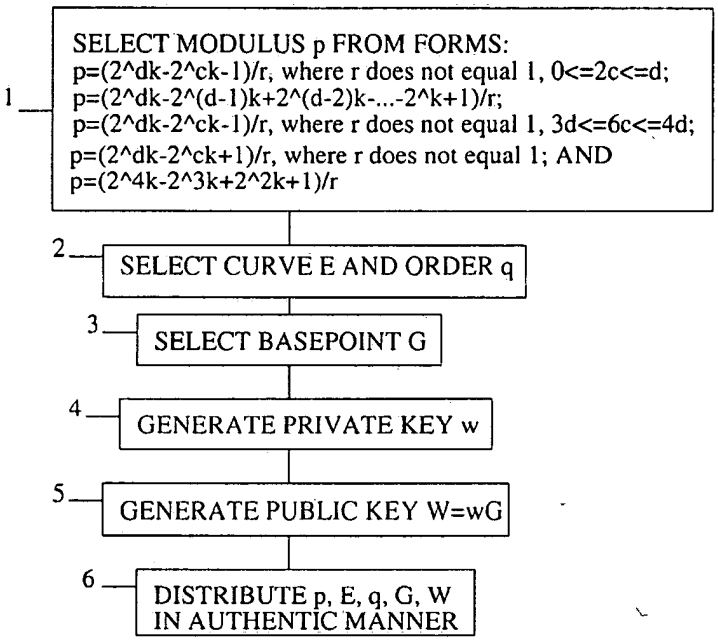

FIG. 1

"REPLACEMENT SHEET"

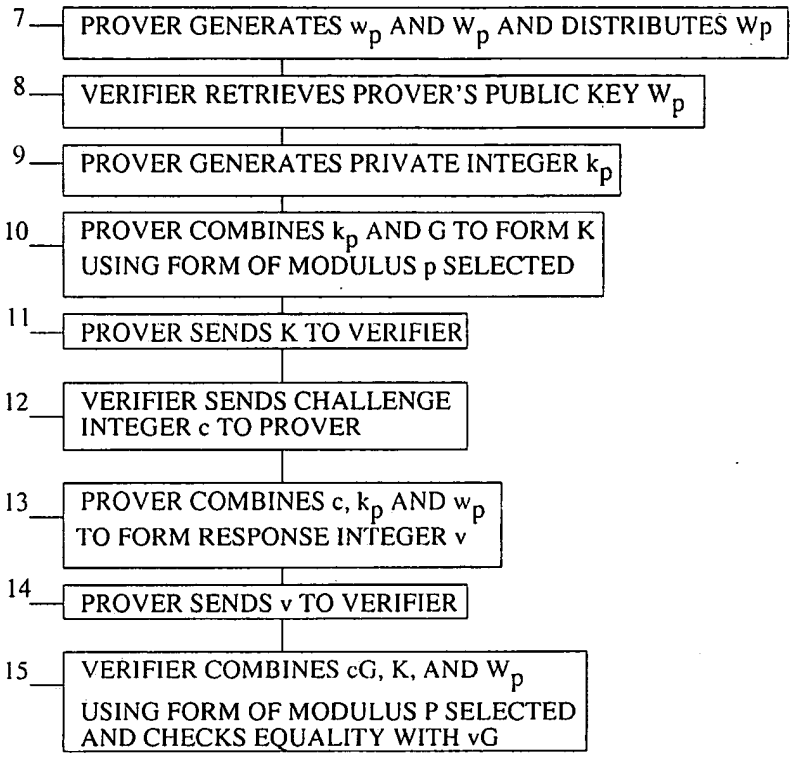

FIG. 2

"REPLACEMENT SHEET"

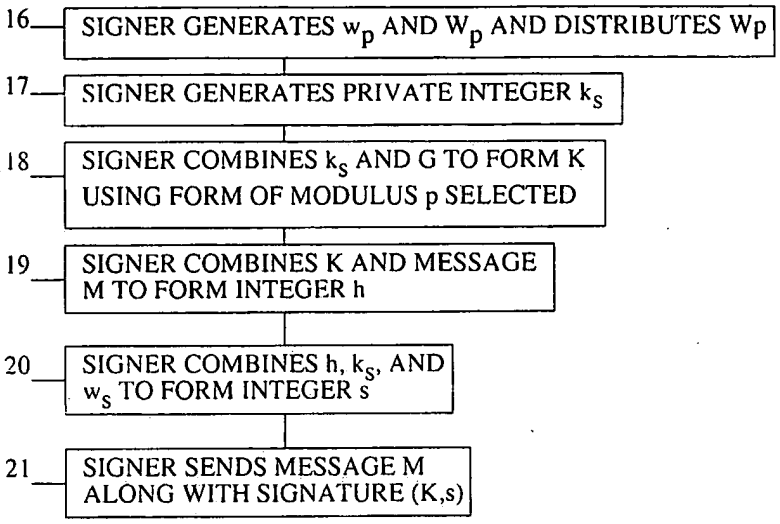

FIG. 3

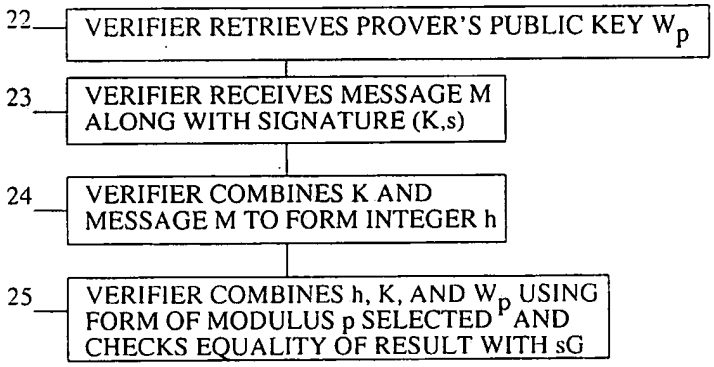

FIG. 4

"REPLACEMENT SHEET"

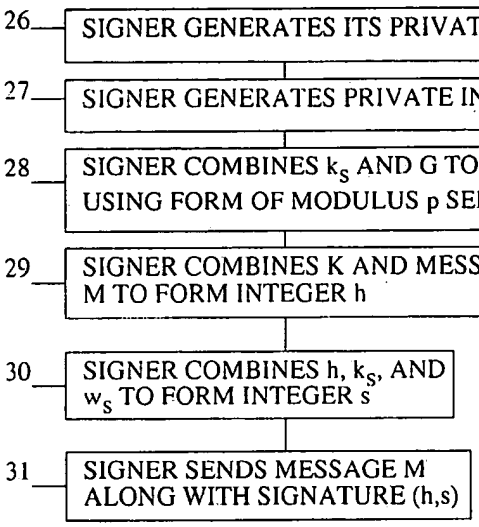

FIG. 5

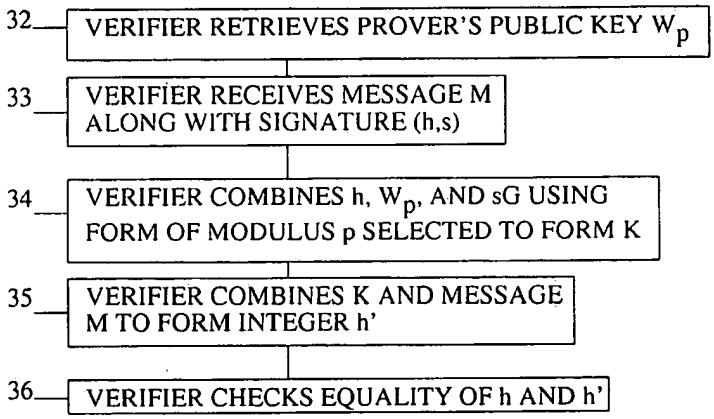

FIG. 6

Conclusion

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tamara Teslovich whose telephone number is (571) 272-4241. The examiner can normally be reached on Mon-Fri 8-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on (571) 272-3868. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).